What is claimed is:

1. A method, by which a terminal (10), enabled for handling data-protocol services, is dynamically configured for the data-protocol services specific to a service provider in a secure way based on a chain of trust so as to be able to connect said terminal (10) to an IP backbone network via a network (16), which provides said data-protocol services and which is provided by said service provider, comprising the steps of:

sending (42, 42a) an access-request signal (30, 30a) to the network (16) by the terminal (10) for connecting to a help-portal server (24, 24a) of said network (16) and for requesting a provisioning signal (38) or a management session signal (38a) for configuring the terminal (10); and

forwarding (52, 52a) the access-request signal (30, 30a) to the help-portal server (24, 24a) by the terminal (10) using a well-known uniform resource locator (URL) and a trusted access point node (20, 20a) in order to provide the provisioning signal (38) or the management session signal (38a) to the terminal (10).

2. The method of claim 1, wherein said data-protocol services specific to said service provider are provided by a general packet radio service.

3. The method of claim 1, wherein the access-request signal (30, 30a) is sent by a browser user agent block (12) of the terminal (10).

4. The method of claim 1, wherein the well-known uniform resource locator (URL) is allowed by an access control profile of the terminal (10).

5. The method of claim 1, further comprising the step of:

sending (58, 58a) the provisioning signal (38) or the management session signal (38a) to the terminal (10) for configuring the terminal (10).

6. The method of claim 5, wherein the provisioning signal (38) or the further provisioning signal (38a) is sent over an IP bearer or sent using a short message service (SMS) protocol.

7. The method of claim 6, wherein said provisioning signal (38) is sent over the IP bearer using a hyper text transfer protocol (HTTP) or a hyper text transfer protocol secure (HTTPS).

8. The method of claim 5, wherein said provisioning signal (38) is sent over the air (OTA).

9. The method of claim 1, wherein after the step of sending (42, 42a) the access-request signal (30, 30a), further comprising the steps of:

identifying (46, 46a) to the terminal (10) the trusted access point node name by a trusted home location register (HLR) (18, 18a) of the network (16);

forwarding (47, 47a) the access-request signal (30, 30a) to the trusted access point node (20, 20a) by the terminal (10);

identifying (48, 48a) to the terminal (10) a trusted domain name service server (22) of the network (16) by the trusted access point node (20, 20a);

forwarding said access-request signal (30, 30a) to the trusted domain name service (DNS) server (22, 22a) by the terminal (10);

forwarding (50, 50a) said access-request signal (30, 30a) by the terminal (10) to the trusted domain name service (DNS) server (22, 22a) for identifying an address mapping for the help-portal server (24, 24a); and

identifying (51, 51a) said address mapping to the terminal (10) by the trusted domain name service server (22, 22a).

10. The method as in claim 9, wherein a security of configuring the terminal (10) is ensured by means of the chain of trust built by the trusted home location register (18, 18a), by the well-known access point node name for accessing the trusted access

point node (20), by the trusted access point node (20, 20a), by the trusted domain name service server (22, 22a) and by the well-known uniform resource locator.

11. The method of claim 1, wherein after the step of forwarding (52, 52a) the access-request signal (30, 30a) to the help-portal server (24, 24a), the method further comprises the steps of:

sending (52, 52a) user authentication request signals (32a, 32b) to an authentication block (26) of the network (16) or to the terminal (10) or to both, the authentication block (26) and the terminal (10), respectively, by the help-portal server (24, 24a), and receiving authentication confirmation signals (34a or 34b) back from the authentication block (26) or from the terminal (10), respectively, or from both, the authentication block (26) and the terminal (10); and

determining if the terminal (10) is authentic by the help-portal server (24, 24a) based on the authentication confirmation signals (34a or 34b).

12. The method of claim 11, wherein said access-request signal (30) contains user identification information, a generic uniform resource locator (URL) request for the help-portal server (24), and a well-known access point node (APN) name for accessing the trusted access point node (20) or a wildcard access point node (APN).

13. The method of claim 12, wherein if it is determined that the terminal (10) is authentic, the method further comprises the steps of:

sending (56) a triggering signal (36) to a provisioning server (28) by the help-portal server (24); and

sending (58) a provisioning signal (38) by the provisioning server (28) to the terminal (10) and so configuring said terminal (10).

14. The method of claim 11, wherein said access-request signal (30a) contains user identification information, a generic uniform resource locator (URL) request for the help-portal server (24a) and for a device management server (28a), a well-known

access point node name for accessing the trusted access point node (20a) or a wildcard access point node (APN).

15. The method of claim 14, wherein if it is determined that the terminal (10) is authentic, the method further comprises the steps of:

sending (60) an initial provisioning triggering signal (27) to a device management server (28a) for initial provisioning; and

sending (62) a further triggering signal (33) by the help-portal server (24a) to an initialization content handler (15) of the terminal (10), said further triggering signal (33) containing a proxy address and a password for connecting to the device management server (28a).

16. The method of claim 15, further comprising the step of:

determining (64) if the further triggering signal (33) contains an instruction of making a connection to the device management server (28a) by the terminal (10).

17. The method of claim 16, wherein if the further triggering signal (33) contains the instruction for making the connection to the device management server (28a) by the terminal (10), the method further comprises the steps of:

sending (68) a start signal (35) to a device management agent block (17) of the terminal (10) by the initialization content handler block (15);

sending (70) a further access-request signal (37) containing a network access authentication to the device development server (28a) by the device management agent block (17); and

sending (58a) the management session signal (38a) by the device development server (28a) to the terminal (10) for further configuring the terminal (10).

18. The method of claim 1, wherein before the step of sending (42, 42a) the access-request signal (30, 30a) to the network (16), the method further comprises the step of:

starting the browser user agent (12) by a starting signal (31) from the user (14).

19. A cellular communication system (11) comprising:

a terminal (10), enabled for handling data-protocol services and dynamically configured for the data-protocol services specific to a service provider in a secure way based on a chain of trust, responsive to a provisioning signal (38) or to a management session signal (38a) for configuring the terminal (10), for providing an access-request signal (30, 30a); and

a network (16) provided by said service provider, responsive to the access-request signal (30, 30a), for providing the data-protocol services specific to a service provider, for forwarding the access-request signal (30, 30a) to a help-portal server (24, 24a) using a well-known uniform resource locator (URL) and a well-known access point node name, for providing the provisioning signal (38) or the management session signal (38a) to the terminal (10) to perform said configuring and for enabling after said configuring a connection of said terminal (10) to an IP backbone network via the network (16).

20. The cellular communication system (11) of claim 19, wherein the well-known uniform resource locator (URL) is allowed by an access control profile of the terminal (10).

21. The cellular communication system (11) of claim 19, wherein said data-protocol services specific to said service provider are provided by a general packet radio service.

22. The cellular communication system (11) of claim 19, wherein the terminal (10) comprises:

a browser user agent block (12), responsive to a starting signal from a user (14), for providing the access-request signal (30, 30a) to the network (16).

23. The cellular communication system (11) of claim 19, wherein the network (16) comprises:

a help-portal server (24, 24a), responsive to the access-request signal (30, 30a) and to one or both authentication confirmation signals (34a, 34b), for providing a triggering signal (36), or an initial provisioning triggering signal (27) and a further triggering signal (33);

a trusted domain name service (DNS) server (22a, 22b), responsive to the access-request signal (30, 30a) from the terminal (10), for identifying to the terminal (10) an address mapping for the help-portal server (24, 24a);

a trusted access point node (20, 20a), responsive to the access-request signal (30, 30a), for providing to the terminal (10) the trusted domain name service (DNS) server (22a, 22b);

a home location register (18, 18a), responsive to the access-request signal (30, 30a), for providing the trusted access point node (20) to the terminal (10); and optionally

an authentication block (26), responsive to an authentication request signal (32b), for providing the authentication confirmation signal (34b) to the help-portal server (24, 24a).

24. The cellular communication system (11) of claim 23, wherein a security of configuring the terminal (10) is ensured by means of the chain of trust built by the trusted home location register (18, 18a), by the well-known access point node name for accessing the trusted access point node (20), and further built by the trusted access point node (20, 20a), by the trusted domain name service server (22, 22a) and by the well-known uniform resource locator.

25. The cellular communication system (11) of claim 23, wherein said access-request signal (30) contains user identification information, a generic uniform resource locator (URL) request for the help-portal server (24), and a well-known access point node (APN) name for accessing the trusted access point node (20) or a wildcard access point node (APN).

26. The cellular communication system (11) of claim 25, wherein the terminal (10) further comprises:

a provisioning server (28), responsive to the triggering signal (36) by the help-portal server (24), for providing the provisioning signal (38) to the terminal (10).

27 The cellular communication system (11) of claim 23, wherein said access-request signal (30a) contains user identification information, a generic uniform resource locator (URL) request for the help-portal server (24a) and for a device management server (28a), a well-known access point node name for accessing the trusted access point node (20a) or a wildcard access point node (APN).

28. The cellular communication system (11) of claim 27, wherein the network (16) further comprises:

a device management server (28a), responsive to the access-request signal (30a) and to a further access-request signal (37) containing a network access authentication, for providing the management session signal (38a) to the terminal (10) for configuring the terminal (10).

29. The cellular communication system (11) of claim 28, wherein the terminal (10) further comprises:

an initialization content handler (15), responsive to the further triggering signal (33) containing a proxy address and a password for connecting to the device management server (28a), for providing a start signal (35); and

a device management agent block (17), responsive to the start signal (35), for providing the further access-request signal (37).

30. The cellular communication system (11) of claim 19, wherein the provisioning signal (38) is sent over an IP bearer or sent using a short message service (SMS) protocol.

31. The cellular communication system (11) of claim 30, wherein said provisioning signal (38) is sent over the IP bearer using a hyper text transfer protocol (HTTP) or a hyper text transfer protocol secure (HTTPS).

32. The cellular communication system (11) of claim 30, wherein said provisioning signal (38) is sent over the air (OTA).

33. A computer program product comprising: a computer readable storage structure embodying computer program code thereon for execution by a computer processor with said computer program code characterized in that it includes instructions for performing the steps of the method of claim 1 indicated as being performed by a terminal (10) or by a network (16) or by both the terminal (10) and the network (16).